



# Department of Homeland Security Daily Open Source Infrastructure Report for 06 June 2006

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

## Daily Highlights

- The Associated Press reports a federal appeals court has blocked regulatory approval to store radioactive waste at the Diablo Canyon nuclear power plant in San Luis Obispo County, California, ruling that federal regulators must first consider the likelihood of a terrorist attack. (See item [6](#))
- The Los Angeles Times reports a looming doctor shortage in at least a dozen specialties threatens to create a national healthcare crisis by limiting access to physicians, jeopardizing quality, and accelerating cost increases. (See item [23](#))

### DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *June 04, Dallas Morning News* — **Gulf refineries, production still haven't recovered.** The energy industry has yet to completely recover from the hurricanes that swept through the Gulf of Mexico last year. Major energy operations still need repairs, and about ten percent of offshore oil and gas production remains offline. The hurricane season this year, which started Thursday, June 1, is expected to deliver even more harsh blows to production and refineries, even with new industry practices and months of preparation. The bottom line: More price spikes appear likely, though officials hope the planning will translate into shorter outages this

time around. Government forecasters expect a heavier than normal hurricane season, though not as strong as last year's. Consumers' energy prices would rise sharply again, if storms this year knock out any pipelines or refineries. Since autumn, companies have been upgrading infrastructure such as mooring systems and preparing backup power units. About half the offshore production platforms are expected to be strengthened by the end of the hurricane season. Mobile drilling rigs have been equipped with so-called black box devices to study the equipment, if motors fail. Satellite phones and text-messaging devices used last year are being supplemented by short-wave radio systems and enhanced fiber-optic lines.

Source: <http://www.journalstar.com/articles/2006/06/04/business/doc4480b4460af81364834341.txt>

2. *June 04, Associated Press* — **Federal agency orders evacuation of mines in Knott County, Kentucky.** The Mine Safety and Health Administration (MSHA) has ordered that three eastern Kentucky mines be evacuated after a seal breach was discovered in one of the mines. No one was hurt because of the breach, which was found at the Consol of Kentucky Incorporated Jones Fork E-3 Mine in Knott County. MSHA says two adjacent mines — Ember Contracting Number 10 mine and Abundance Coal Incorporated Number 1 mine — have been closed. MSHA's acting administrator says the agency is requiring alternative seals to be evaluated. Source: [http://www.lex18.com/Global/story.asp?S=4979618&nav=menu203\\_1\\_3](http://www.lex18.com/Global/story.asp?S=4979618&nav=menu203_1_3)
3. *June 04, Associated Press* — **Bird, storm black out thousands in Tucson, Arizona.** First it was a bird, then it was the wind. The double whammies just hours apart Saturday, June 3, caused more than 50,000 Tucson Electric Power (TEP) customers to lose service across Tucson, AZ. Nearly two dozen utility poles were snapped by the wind. The first power outage occurred at about 4:15 p.m. MDT when a bird flew into a TEP substation and caused a short, cutting the power to areas stretching from Midtown to the South Side, said Joe Salkowski, a utility spokesperson. More than 35,000 customers lost power for about an hour. A few hours later, fast-moving thunderstorms ripped through Tucson, bringing winds that brought down power lines and left more than 12,000 customers without electricity. In another outage, 12,000 customers were without electricity late Saturday, Salkowski said. Source: [http://news.yahoo.com/s/azstar/20060604/lo\\_azstar/birdstormblackoutthousandscrewsworkintothelateeveningtofixdualeventdamage](http://news.yahoo.com/s/azstar/20060604/lo_azstar/birdstormblackoutthousandscrewsworkintothelateeveningtofixdualeventdamage)
4. *June 04, Associated Press* — **Power vandals charged.** Two Sisseton, SD men are scheduled to stand trial August 1 on charges they shot holes in an Otter Tail Power Co. transformer in northeast South Dakota, causing an outage and at least \$100,000 in damage. The crime happened between March 1 and April 16 at a substation just north of Sisseton. About 20 rounds were fired from a .22-caliber rifle into the transformer, said Kevin Kouba of Otter Tail. The resulting outage left about 600 customers without power for about a half hour, he said. Source: [http://www.aberdeennews.com/mld/aberdeennews/news/14738427.htm?source=rss&channel=aberdeennews\\_news](http://www.aberdeennews.com/mld/aberdeennews/news/14738427.htm?source=rss&channel=aberdeennews_news)
5. *June 03, Green Bay Press Gazette (WI)* — **Nuclear disaster drills staged.** The Emergency Operations Facility for Dominion Resources Inc. simulated an emergency exercise on Thursday, June 1, for the Kewaunee Power Station, a nuclear plant located in Carlton, MI. A dozen plant employees sat in front of four large screens on the wall showing simulated data from the plant. Operators dealt with several simulated issues simultaneously — ranging from a

control rod/reactor fuel problem to ways to keep the reactor cool after three feed–water pumps were rendered unavailable following an earthquake and other events. Other employees gathered information about the event and preparing statements for the media. The building, a \$1.8 million investment for Dominion required by federal regulations, is designed to be a central gathering point for plant emergency teams, federal, state and local emergency officials, and the media.

Source: <http://www.greenbaypressgazette.com/apps/pbcs.dll/article?AI=D=/20060603/GPG03/606030471/1247/GPGbusiness>

6. *June 03, Associated Press* — **Nuclear regulators told to review nuclear facility terrorist threat.** A federal appeals court blocked regulatory approval to store radioactive waste at the Diablo Canyon nuclear power plant in San Luis Obispo County, CA, ruling Friday, June 2, that federal regulators must first consider the likelihood of a terrorist attack. The 9th U.S. Circuit Court of Appeals, in the first ruling of its kind, disagreed with the Nuclear Regulatory Commission's (NRC) 2003 finding that an attack was "remote and speculative" and therefore the possibility need not be seriously considered. The plant is building new stainless steel and cement storage facilities because the current waste repository at the Pacific Gas & Electric Co. site is filling up. The court said the NRC could not justify its so-called "top to bottom" security review of the nation's nuclear installations, while it simultaneously declared that the risk of a terrorist attack cannot be quantified, Judge Sidney Thomas wrote for the three-judge panel.
- Source: [http://www.contracostatimes.com/mld/cctimes/news/politics/14\\_733177.htm](http://www.contracostatimes.com/mld/cctimes/news/politics/14_733177.htm)

[\[Return to top\]](#)

## **Chemical Industry and Hazardous Materials Sector**

Nothing to report.

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

7. *June 02, Air Force Times* — **U.S. Army's light aircraft to be ready by October 2009.** The U.S. Army will be able to field its future light cargo aircraft by the end of fiscal 2009 if \$109 million earmarked for the project by the Senate Armed Forces Committee comes through during this budget cycle, the director of Army aviation said Friday, June 2. The plane's primary purpose will be to ferry troops and supplies to the frontlines in a way the Army's current aircraft can't, said Brigadier General Stephen D. Mundt. The plane should be able to land on a 2,000-foot runway, Mundt said. The Army is soliciting industry bids for the joint cargo aircraft. Officials intend to make a selection in February 2007 and award a contract by the end of that month. The planes should be tested by select units by fiscal 2008 and fielded by the end of fiscal 2009.
- Source: <http://airforcetimes.com/story.php?f=1-292925-1844796.php>
8. *June 02, Federal Computer Week* — **DISA seeks input on insider threat tools.** The Defense Information Systems Agency (DISA) wants industry input on tools that could counter insider threats to Department of Defense (DoD) information systems. DISA said traditional efforts to

secure networks focus on outside threats, but insiders pose an equally damaging threat and they can access DoD networks without detection by the security systems. DISA, in a request for information (RFI) released Thursday, June 1, said it's looking for an insider threat focused observation tool that could be deployed on selected host DoD machines to aggressively gather and analyze data on inside threats. The due date for RFI responses is Wednesday, July 5.  
Source: <http://www.fcw.com/article94741-06-02-06-Web>

[[Return to top](#)]

## **Banking and Finance Sector**

9. *June 05, Boca Raton News (FL)* — **With advanced planning, Florida banks are ready for hurricane season.** Boca Raton, FL, banks have taken steps to make sure they can deal with weather-related disasters and other emergencies. Among commercial banks, SunTrust branches have established hurricane policies designed to help both employees and customers. SunTrust employees undergo extensive training prior to hurricane season in order to respond effectively during an emergency. Employees are encouraged to use a special Website, developed by SunTrust, that explains various hurricane protocols the bank has established. If a hurricane strikes, branch managers will follow up afterwards with employees to determine their status. All SunTrust branches are equipped with emergency generators in case of power failure. ATM machines will be stocked with money and will work as long as the branch they are located at has power. Some branches will install portable ATM machines that don't require power to operate. Independent community financial institutions, such as First Southern Bank, have also come up with preventative measures. Besides its own emergency generator, First Southern has backup storage of client data at another facility — in case the information disappears locally. Peter Mottek of First Southern said, "Regardless of what happens, our aim is to be operating again by 72 hours after the storm."  
Source: <http://www.bocaratonnews.com/index.php?src=news&prid=15633&category=BUSINESS%20NEWS>

10. *June 04, Associated Press* — **Theft of data went further, Veterans Affairs Department discloses.** Personal data on up to 50,000 active Navy and National Guard personnel were among what was stolen from a Veterans Affairs Department (VA) employee last month, the government said Saturday, June 3, in a disclosure that went beyond what it had reported. VA Secretary Jim Nicholson said his agency had discovered after an internal investigation that the names, Social Security numbers, and birthdates of up to 20,000 National Guard and Reserve personnel who were on at least their second active-duty call-up were "potentially included." In addition, the same information on as many as 30,000 active-duty Navy personnel who completed their first enlistment term before 1991 was also believed to have been stored on a laptop and computer disks stolen on Wednesday, May 3 from the home of a VA data analyst.  
Source: [http://www.nytimes.com/2006/06/04/washington/04vets.html?\\_r=1&oref=slogin](http://www.nytimes.com/2006/06/04/washington/04vets.html?_r=1&oref=slogin)

11. *June 04, Sydney Morning Herald (Australia)* — **Gangs using Aussie kids to steal millions.** Police have smashed an international fraud gang that used school-aged children in Sydney to launder money stolen from unwitting victims' bank accounts. The gang used phishing to get people's online bank account details and passwords. The Triad gang — which has been traced as far as Malaysia and Russia — then used the codes to hack into victims' accounts via the

Internet before transferring the funds to other accounts. Teenagers were recruited as "mules" to receive the stolen money in their own personal bank accounts. They would then pass the money, minus a commission, to "bagmen" for the gang, who wired the money to the gang's bosses overseas. A total of 61 people were robbed of more than \$600,000. Australian High Tech Crime Centre Federal Agent Kevin Zuccato warned that Internet criminals were becoming very sophisticated, targeting emails with believable language and messages. "One created a mock Reserve Bank message asking people to assist the bank to protect against terrorism financing," Zuccato said.

Source: <http://www.smh.com.au/articles/2006/06/03/1148956585189.html?page=fullpage#contentSwap1>

12. *June 02, Sentinel (PA)* — **Stolen laptop had information about Giant retirees.** Personal information for an undisclosed number of Giant Food Stores retirees may have been on a laptop computer that was lost or stolen Tuesday, May 2, on an airline flight, Giant officials say. "Right now there hasn't been" a case of identity theft. "It's a simple data breach," says Barry Scher, spokesperson for Giant parent company Ahold USA. A Giant vendor working on company pension plans had placed the laptop in checked baggage, a May 24 letter from Ahold to the affected retirees, says. Names, Social Security numbers, birth dates, benefit amounts, and administrative information was in a file in the laptop, the letter says. No financial or medical benefit information was in the file, which was not encrypted or password protected, although the laptop was password protected, the letter says.

Source: <http://www.cumberlink.com/articles/2006/06/05/news/news19.txt>

[[Return to top](#)]

## **Transportation and Border Security Sector**

13. *June 05, Associated Press* — **JetBlue wins air-ground wireless license.** JetBlue Airways Corp. won a government auction Friday, June 2, for wireless spectrum that could be used to provide in-flight telephone, Internet, or entertainment services. The winning bid of \$7.02 million was placed through New York-based JetBlue's entertainment subsidiary, LiveTV LLC, which provides DirecTV service on JetBlue flights. The 1-megahertz frequency band sold by the Federal Communications Commission (FCC) is nationwide and not limited to JetBlue aircraft, opening the possibility that LiveTV will offer the service to other airlines. A larger swath of spectrum, 3-megahertz of bandwidth, was won by AirCell Inc. of Louisville, CO, with backing by Ripplewood Holdings LLC, a New York-based private equity firm. Both bands sold in the auction are currently used by Verizon Airfone, a subsidiary of Verizon Communications Inc. The Boeing Co. operates a competing in-flight broadband service, Connexion, for international carriers. It uses satellite links instead of air-to-ground communications.

Source: [http://www.usatoday.com/travel/flights/2006-06-05-jetblue-wireless\\_x.htm](http://www.usatoday.com/travel/flights/2006-06-05-jetblue-wireless_x.htm)

14. *June 05, Reuters* — **IATA sees \$3 billion airline losses in 2006.** Global airlines are set to lose \$3 billion in 2006, barely recovering from \$3.2 billion of losses in 2005 as they contend with rising fuel bills, industry group International Air Transport Association (IATA) said on Monday, June 5. IATA, which represents 261 airlines handling 94 percent of the world's scheduled air traffic, had previously forecast \$2.2 billion of combined losses in 2006. But oil



prices have hit new peaks while the dollar's decline also hurts many airlines. Fuel is expected to make up 26 percent of airlines' average costs in 2006 compared with 22 percent last year. In order to make money, airlines need on average to fill 63.3 percent of their available capacity by weight in 2006, but are only expected to manage 62.4 percent, IATA said.

Source: [http://www.usatoday.com/travel/flights/2006-06-05-airline-losses\\_x.htm](http://www.usatoday.com/travel/flights/2006-06-05-airline-losses_x.htm)

15. *June 05, Transportation Security Administration* — **Explosives detection capability expanded at Kansas City International Airport.** The Transportation Security Administration (TSA) on Monday, June 5, announced the deployment of five Reveal explosives detection systems (EDS) for screening checked baggage at Kansas City International Airport (MCI). The Reveal CT-80 machines are smaller in size and are less than half the price of other EDS machines currently in use at commercial airports nationwide. In 2005, TSA deployed eight Reveal machines for operational field testing and evaluation at three airports: Gulfport-Biloxi International Airport (MS), Newark Liberty International Airport (NJ) and John F. Kennedy International Airport (NY). The field tests lasted from 30 to 45 days at each airport and provided TSA with the opportunity to evaluate the machine's effectiveness in an airport environment as well as its impact on security and customer service. Following the success of the pilot program, 18 other airports are scheduled to receive Reveal equipment this year. Those airports include Albany, NY, Billings, MT, Norfolk, VA, Charleston, SC, Atlantic City, NJ, Memphis, TN, and Bangor, ME.

Source: <http://www.tsa.gov/public/display?theme=44&content=09000519801ec63b>

16. *June 05, New York Times* — **Canadian border proves difficult to secure.** Tighter border controls between the United States and Canada are likely to be less useful than better domestic intelligence and information-sharing in detecting homegrown terrorist plots in North America, terrorism experts said on Sunday, June 4. John O. Brennan, former director of the National Counterterrorism Center and a former career Central Intelligence Agency officer, said that while improved border technology and a planned requirement that Canadian visitors carry passports might help, there was no chance of stopping all potential terrorists from crossing a 4,000-mile border that includes huge swaths of forest and the Great Lakes. He said, the lesson for the United States is the value of careful, patient intelligence collection to detect possible threats. Meanwhile, according to Canadian authorities, the suspected fertilizer bomb plot that led to the arrest Saturday in Ontario of 17 men, most of them Canadian citizens of South Asian origin, appeared to follow the pattern of successful terrorist attacks in Madrid in 2004 and in London last year.

Source: [http://www.nytimes.com/2006/06/05/world/americas/05border.html?\\_r=1&oref=slogin](http://www.nytimes.com/2006/06/05/world/americas/05border.html?_r=1&oref=slogin)

17. *June 05, Associated Press* — **New carrier shaking up travel in Hawaii.** On Friday, June 9, "Go!" airlines will launch its service, becoming the third inter-island jet carrier in Hawaii. The low-cost carrier is a venture of Mesa Air Group Inc., the largest company to enter the exclusive inter-island market dominated for decades by Hawaiian and Aloha airlines. That's not good news for Hawaiian and Aloha, both recently emerging from Chapter 11 bankruptcy protection and under pressure to perform for new investors. And, Aloha and Hawaiian have paid close attention to Mesa, quickly matching the low-cost carrier's every promotion and discount, despite soaring fuel costs. Phoenix-based Mesa is one of the nation's largest regional carriers with 182 jets, 5,000 employees and annual revenues exceeding \$1 billion. It flies to more than

170 cities under the America West Express, Delta Connection, United Express names. Experts say Mesa is taking a gamble by creating and operating its own airline, instead of sticking to its traditional, low-risk business model of providing connecting service for other carriers. Go! plans to operate 32 flights per day, using three 50-passenger Canadair regional jets. Flights will double when additional aircraft are added June 30.

Source: [http://www.usatoday.com/travel/flights/2006-06-05-hawaii-far-e-war\\_x.htm](http://www.usatoday.com/travel/flights/2006-06-05-hawaii-far-e-war_x.htm)

18. *June 04, Associated Press* — **Japan Airlines to join Oneworld Alliance.** Japan Airlines will join the Oneworld Alliance -- which includes AMR Corp.'s American Airlines and British Airways PLC -- early next year, the group said Sunday, June 4. Japan Airlines had not previously joined a major international carrier alliance, though it has code-sharing agreements allowing it to share flights with rivals. The move will allow JAL, Japan's biggest carrier, to expand its flight network and make it easier for passengers to connect to flights of other airlines. The group now serves 134 nations and 599 destinations. Other Oneworld members are Qantas, Cathay Pacific, Iberia, LAN, Finnair, and Aer Lingus. Royal Jordanian is expected to join.

Source: [http://biz.yahoo.com/ap/060604/japan\\_airlines\\_alliance.html?.v=2](http://biz.yahoo.com/ap/060604/japan_airlines_alliance.html?.v=2)

[[Return to top](#)]

## **Postal and Shipping Sector**

Nothing to report.

[[Return to top](#)]

## **Agriculture Sector**

19. *June 05, Agricultural Research Service* — **Scientists vaccinating bison.** Agricultural Research Service (ARS) scientists in Ames, Iowa, have been firing vaccine-filled projectiles at close range into bison's muscle tissues. The activity is part of testing ballistic approaches to vaccinating wildlife against brucellosis, an infectious disease of both animals and humans. Veterinary medical officer Steven Olsen of the ARS National Animal Disease Center (NADC) in Ames, with colleagues at Colorado State University in Fort Collins, are seeking better ways to remotely inject free-ranging bison with RB51, the most effective vaccine available against brucellosis in cattle. Brucellosis is a bacterial infection that in animals induces abortions, decreases fertility and reduces milk production. The bacteria can also be transmitted to humans -- through contact with infected animals or consumption of unpasteurized dairy products -- and cause undulant fever, an affliction characterized by severe flu-like symptoms. Brucellosis has been nearly eradicated in the U.S., but outbreaks among wildlife have concerned cattle producers because cattle can get the disease through close contact with infected animals.

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

[[Return to top](#)]

## **Food Sector**

20. *June 05, USAgNet* — **South Korea may delay resuming U.S. beef imports.** South Korea could push back its plan to resume U.S. beef exports from later this week to next month because of problems Seoul sees with U.S. meat processors, the agriculture minister said on Monday, June 5. "U.S. beef processing facilities do not meet the standards suggested by the South Korean government. So the first shipment of U.S. beef to South Korea may not be allowed this month," Park Hong-soo, South Korea's agriculture minister, told reporters. South Korea banned the imports more than two years ago because of mad cow disease fears. South Korea had said last month it would resume U.S. beef imports from Wednesday, June 7, after it announces a list of approved U.S. beef processors. Park did not give further details about what the ministry saw as the shortcomings at the U.S. meat processors.

Source: <http://www.usagnet.com/story-national.cfm?Id=1058&yr=2006>

[[Return to top](#)]

## **Water Sector**

21. *June 05, Associated Press* — **Denver Water drafts plan to cut use twenty-two percent.**

Denver Water has laid out a \$400 million plan aimed at slashing customers' annual water use by 22 percent over the next 10 years. The Colorado utility drafted the plan in hopes of reducing annual consumption by 16.7 billion gallons by 2016. "Our system is able to meet our current needs, but in the future, it's going to take more supply, more conservation — or both — to be able to provide for a rapidly urbanizing Front Range," said Denver Water Commissioner Tom Gougeon. One proposal would require builders to meet certain standards for water efficiency before the utility would hook up a new home to the water system. Another would require audits of existing homes before they are sold and requiring the replacement of leaky fixtures. Municipal and commercial customers might have to add irrigation water meters and remove park lawns.

Source: [http://cbs4denver.com/topstories/local\\_story\\_156080603.html](http://cbs4denver.com/topstories/local_story_156080603.html)

[[Return to top](#)]

## **Public Health Sector**

22. *June 05, Bloomberg* — **Bird flu fighters need money to help contain virus.** The World Organization for Animal Health and United Nations agencies, including the Food and Agriculture and World Health Organizations, said they have received less than half the \$1.9 billion pledged by donors at a conference in January. Since then, the H5N1 avian influenza virus has infected animals in 36 new countries, resulting in human cases in four nations. The lack of funding may derail efforts to control H5N1. Africa alone needs about \$500 million, said Bernard Vallat, director general of the animal health organization. Governments are under pressure to stem poultry outbreaks, which create opportunity for human infection and increase the risk that H5N1 will mutate into a pandemic form. The virus has infected a new person every other day this year, killing almost two thirds of them.

Source: <http://www.bloomberg.com/apps/news?pid=10000101&sid=a4U1iJ0UpSDM&refer=japan>



23. *June 04, Los Angeles Times* — **Physician shortage looms.** A looming doctor shortage threatens to create a national healthcare crisis by limiting access to physicians, jeopardizing quality, and accelerating cost increases. Across the country, patients are experiencing or soon will face shortages in at least a dozen physician specialties, including cardiology and radiology. It may be too late to head off havoc for at least the next decade, experts say, given the long lead time to train surgeons and other specialists. The number of medical school graduates has remained virtually flat for a quarter century, because the schools limited enrollment out of concern that the nation was producing too many doctors. But demand has exploded, driven by population gains, a healthy economy and a technology-driven boom in physicians' repertoires. Over the next 15 years, aging baby boomers will push urologists, geriatricians and other physicians into overdrive. Yet, much of the nation's physician workforce also is aging. A third of the nation's 750,000 active, post-residency physicians are older than 55. By 2020, physicians are expected to retire at a rate of 22,000 a year, up from 9,000 in 2000. That is only slightly less than the number of doctors who completed their training last year.

Source: <http://www.latimes.com/business/la-fi-doctors4jun04%2C0%2C1528090.story?coll=la-home-headlines>

24. *June 01, CIDRAP News* — **European Union reports H5N1 cases in wild birds.** The European Commission (EC) reported Wednesday, May 31, that 741 cases of H5N1 avian influenza have been detected among about 60,000 wild birds tested in European Union (EU) states since February. The EC presented its data during the United Nations Food and Agriculture Organization (FAO)/World Organization for Animal Health (OIE) International Scientific Conference on Avian Influenza and Wild Birds. The EC and the Community Reference Laboratory for Avian Influenza in the United Kingdom, began testing wild birds in all EU states in July 2005. The EC, said that though final figures are still being collected for recent months, 741 wild birds in 13 member states tested positive for highly pathogenic avian influenza between February and May 21 of this year. Most of those were confirmed to be H5N1 cases. About 60,000 birds were tested in that period, and about 99,000 over the entire 10 months of testing. Germany had the most cases, with 326, followed by Austria (117), Poland (64), France (62), and Denmark (42), the EC reported.

Source: <http://www.cidrap.umn.edu/cidrap/content/influenza/avianflu/news/jun0106birds.html>

[[Return to top](#)]

## **Government Sector**

25. *June 04, CNN* — **Man arrested trying to jump White House fence.** The Secret Service arrested a man who was trying to jump the White House fence carrying a suspicious package on Sunday, June 4. Secret Service spokesperson Tom Mazur said the man, 44-year-old Roger Witmer, was arrested before he made it over the fence. Mazur said Witmer will be charged with unlawful entry, disorderly conduct, and destruction of government property. "Evidently he had in his possession some type of plastic bag and that ended up on the South Lawn at the fence line," said Mazur. He characterized the bag as a "suspicious package" and said the Secret Service was investigating its contents.

Source: <http://www.cnn.com/2006/US/06/04/white.house.jumper/index.html>

26.

*June 02, WTVM (GA)* — **Suspicious powder forces Georgia government center evacuation.**

Just as Columbus, GA, Mayor Bob Poydasheff introduced the new state director of homeland security, the local homeland security office was sent into high gear. A suspicious substance was found inside an envelope in the Superior Court Clerk's Office. Inside the letter was a white powder along with a threatening note. Local homeland security officials quickly blocked off the entire second floor. The Mayor said the situation was controlled with good organization. "That's the whole purpose of my Columbus Regional Homeland Security Board. So that we are all together and people are not going haphazardly all over the place and we responded quickly," says Mayor Poydasheff. The white powder was sent to Atlanta for further testing.

Source: <http://www.wtvm.com/Global/story.asp?S=4981988>

[\[Return to top\]](#)

## **Emergency Services Sector**

27. *June 05, Associated Press* — **Report released on response to London terror attacks.** Flawed emergency planning and communications breakdowns marred the response to last July's London Tube and bus bombings, an official report published Monday, June 5, concludes. The London Assembly's report highlights both the heroism and the confusion of emergency crews responding to the bombs, which killed 52 commuters and four bombers and left about 700 people injured. One of several inquiries into the attacks, the report describes how rescuers' phones and radios failed, and some hospitals relied on staff running to and from bomb sites to gather information. The report includes harrowing testimony by survivors, who gave evidence to London Assembly politicians at a series of private and public sessions. The report makes about 50 recommendations for improvements to emergency response procedures.

Report: [http://www.cabinetoffice.gov.uk/publications/reports/intelligence/isc\\_7july\\_report.pdf](http://www.cabinetoffice.gov.uk/publications/reports/intelligence/isc_7july_report.pdf)

Source: <http://www.cnn.com/2006/WORLD/europe/06/05/uk.bombings.report.ap/>

28. *June 05, Government Accountability Office* — **GAO-06-519: U.S. Tsunami Preparedness: Federal and State Partners Collaborate to Help Communities Reduce Potential Impacts, but Significant Challenges Remain (Report).** The 2004 Indian Ocean tsunami raised questions about U.S. preparedness for such an event. The National Oceanic and Atmospheric Administration (NOAA) leads U.S. detection and warning efforts and partners with federal and state agencies in the National Tsunami Hazard Mitigation Program to reduce tsunami risks. In 2005, Congress appropriated \$17.24 million in supplemental funding to enhance these efforts. This report (1) identifies U.S. coastal areas facing the greatest tsunami hazard and the extent to which potential impacts have been assessed, (2) discusses the effectiveness of the existing federal tsunami warning system, (3) describes efforts to mitigate the potential impacts of tsunamis on coastal communities, and (4) assesses NOAA's efforts to develop long-range plans for federal tsunami programs. The Government Accountability Office (GAO) recommends, among other things, that NOAA take steps to develop software for tsunami loss estimation, conduct periodic end-to-end warning system tests, increase high-risk community participation in its tsunami preparedness program and prepare risk-based strategic plans for its efforts. NOAA reviewed a draft of this report and generally agreed with the findings and recommendations.

Highlights: <http://www.gao.gov/highlights/d06519high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-519>

29. *June 04, ABC News Online (Australia)* — **Radiation vaccination may be possible, say scientists.** Scientists at the University of Pittsburgh School of Medicine say it may soon be possible to vaccinate emergency workers against the effects of a nuclear explosion. In experiments with mice, researchers used a tiny artificial sac to deliver a protective compound to every cell. Twenty-four hours later the mice were exposed to doses of whole body radiation. Those that had been given the gene therapy survived.  
Source: <http://www.abc.net.au/news/newsitems/200606/s1654796.htm>
30. *June 04, Times-Picayune (LA)* — **Guard, police plan storm tactics.** As if preparing for an assault, Louisiana National Guard soldiers and New Orleans police officers hit the streets together Saturday, June 3, to iron out details of how they will evacuate and secure the city when it next faces a powerful hurricane. Kicking off a four-day "tactical exercise without troops," National Guard battalion and company commanding officers joined commanders of the New Orleans Police Department's eight districts. Together, the officials planned to spend the day touring neighborhoods and pinpointing critical sites that about 3,000 National Guard soldiers may be asked to protect, such as drainage pump stations, electric power stations and hospitals. National Guard officials also detailed their plans to send assessment, search-and-rescue and engineering teams from their units across Louisiana into New Orleans within three hours of a storm's passing. The objectives of the joint security effort: to make sure that no citizen of the city of New Orleans dies in a hurricane; to help ensure the quick, orderly evacuation of New Orleans; and to install a police presence in every corner of a city that could be largely emptied of residents.  
Source: <http://www.nola.com/news/t-p/metro/index.ssf?/base/news-15/1149401450165140.xml>
31. *June 02, National Journal* — **DHS seeks to better serve disaster victims with disabilities.** As people flowed out of New Orleans last August during Hurricane Katrina, complaints began flowing in from those with disabilities who were poorly served during the evacuation. By the end of September, in an effort to help the disabled, Department of Homeland Security (DHS) Secretary Michael Chertoff dispatched a team from Washington to join the Federal Emergency Management Agency's recovery operations. Daniel Sutherland, the DHS officer for civil rights and civil liberties who is chairman of the department's Interagency Coordinating Council on Emergency Preparedness and Individuals With Disabilities, said that DHS began implementing changes even before formal policy reviews were completed. The first — and likely most sweeping — of these is establishing a disability section in the disaster headquarters. Other changes will include new operating procedures to address special needs. The DHS coordinating council is also working on recommendations, including ensuring that announcements in emergency shelters are accessible to people who do not hear or see, and providing ways for the disabled to identify their special needs when they register for federal assistance.  
Source: [http://govexec.com/story\\_page.cfm?articleid=34232&dcn=todays\\_news](http://govexec.com/story_page.cfm?articleid=34232&dcn=todays_news)

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

32.

*June 05, Reuters* — **Swedish security police probe suspected Web attacks.** Sweden's domestic intelligence agency said it would probe why the government's Website crashed on Sunday, June 4, amid reports hackers had sought revenge for a crackdown on alleged online piracy. The government Website went off line in the early hours of Sunday. The Internet home page of the national police crashed in similar fashion on Thursday, June 1. The police Website problem came a day after the Pirate Bay Internet page, which the recording industry calls a major source for downloading pirated music and films, was shut by police. Newspaper Aftonbladet quoted a group, called World Wide Hackers, as saying they had arranged an attack on the government's Website.

Source: <http://www.eweek.com/article2/0,1895,1971649,00.asp>

- 33. *June 05, Silicon* — Major spammer pays \$1 million settlement.** A major spammer who was accused of sending up to 25 million e-mails per day has settled a lawsuit with Microsoft and the State of Texas. The settlement has cost Ryan Pitylak \$1 million, as well as the seizure of many of the assets he accumulated during a short-lived career as one of the world's worst spammers. At the peak of his spamming activity, the 24-year-old Texas resident was listed as the world's fourth most prolific spammer by anti-spam group Spamhaus.

Source: <http://www.silicon.com/research/specialreports/thespamreport/0,39025001,39159291,00.htm>

- 34. *June 02, VNUNet* — World Cup streaming to cause network meltdown.** The BBC's decision to stream all its football matches live on the Internet has been greeted with joy by UK fans, but could cause massive headaches for the country's network managers. Roger Mosey, director of sport at the BBC, admitted that there would be a lot of office viewing as some games kick off. However, experts in the networking industry warned that staff using the service could bring UK corporate networks to their knees. Mike Bailey, UK country manager at Ipanema Technologies, explained that network managers need to take note of possible problems to make sure that systems are not adversely affected.

Source: <http://www.vnunet.com/vnunet/news/2157492/bbc-invites-networ k-meltdown>

### Internet Alert Dashboard

#### DHS/US-CERT Watch Synopsis

**Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.**

**US-CERT Operations Center Synopsis:** US-CERT is aware of a buffer overflow vulnerability in Symantec Client Security and Symantec Antivirus Corporate Edition. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary code with SYSTEM privileges. We are not aware of any public exploits at this time. For more information please review the following:

**VU#404910** – Symantec products vulnerable to buffer overflow:

<http://www.kb.cert.org/vuls/id/4049100>

**Symantec Advisory SYM06-010** – Symantec Client Security and Symantec AntiVirus Elevation of Privilege:

<http://securityresponse.symantec.com/avcenter/security/Content/2006.05.25.html>

US-CERT will advise as more information becomes available.

### **Active Exploitation of a Vulnerability in Microsoft Word**

US-CERT is aware of an increase in activity attempting to exploit a vulnerability in Microsoft Word. The exploit is disguised as an email attachment containing a Microsoft Word document. When the document is opened, malicious code is installed on the user's machine. The exploit then attempts to connect to a remote host. More information about the reported vulnerability can be found in the following:

**TRA06-139A** – Microsoft Word Vulnerability:

<http://www.us-cert.gov/cas/techalerts/TA06-139A.html>

**VU#446012** – Microsoft Word buffer overflow:

<http://www.kb.cert.org/vuls/id/446012>

US-CERT recommends the following actions to mitigate the security risks:

Install anti-virus software, and keep its virus signature files up to date. Block executable and unknown file types at the email gateway. Review the workarounds described in Microsoft Security Advisory 919637:

<http://www.microsoft.com/technet/security/advisory/919637.mspx>

Additionally, US-CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. US-CERT will continue to update current activity as more information becomes available.

### **PHISHING SCAMS**

US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US-CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US-CERT.

[http://www.us-cert.gov/nav/report\\_phishing.html](http://www.us-cert.gov/nav/report_phishing.html)

Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. <http://onguardonline.gov/phishing.html>

#### **Current Port Attacks**

--	--



<b>Top 10 Target Ports</b>	1026 (win-rpc), 6881 (bittorrent), 445 (microsoft-ds), 4672 (eMule), 80 (www), 113 (auth), 25 (smtp), 135 (epmap), 139 (netbios-ssn), 53 (domain)
----------------------------	---

Source: <http://isc.incidents.org/top10.html>; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

## **Commercial Facilities/Real Estate, Monument & Icons Sector**

Nothing to report.

[[Return to top](#)]

## **General Sector**

**35. *June 05, Reuters* — Terrorists targeted Canadian landmarks.** The Peace Tower at the center of Ottawa's parliamentary complex and a building at the foot of Toronto's CN Tower were among the targets of a group of home-grown terror suspects arrested over the weekend, Canadian media said Monday, June 5. The group — 17 people have been arrested so far — had the "intent and capability" to launch attacks, Mike McDonell, assistant commissioner of the Royal Canadian Mounted Police, said on Monday. "There is a chance we could be arresting more people. We are following up every lead to the nth degree, and any person that has aided, facilitated or participated in this threat will be arrested," he said. The men and youths were arrested on Friday night and early Saturday, June 3, in a high-profile police swoop that involved 400 officers in and around Toronto, Canada's largest city and its economic powerhouse. Several of the suspects attended the same mosque in a Toronto suburb where a local parliamentarian had complained in the past about the radical views held by some worshippers.

Source: <http://www.cnn.com/2006/WORLD/americas/06/05/canada.terror.targets.reut/index.html>

[[Return to top](#)]

### **DHS Daily Open Source Infrastructure Report Contact Information**

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644 for more information.

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.